UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/688,452	10/16/2000	Craig L. Ogg	40628/RRT/S850	1642

23363   7590   12/12/2003

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER
BACKER, FIRMIN

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 12/12/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.		icant(s)
Office Action Summary	09/688,452		OGG ET AL.
	Examiner		Art Unit
	Firmin Backer		3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2000* .

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-68* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____ .

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)	4)☐ Interview Summary (PTO-413) Paper No(s). _____ .
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5)☐ Notice of Informal Patent Application (PTO-152)
3)☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .	6)☐ Other: .

Response to Amendment

This is in response to an amendment file on September 29th, 2003 for letter for patent

filed on October 16th, 2000 in which claims 1-68 were presented for examination. In the

amendment, claims 1, 30 and 57 have been amended, no claim has been canceled, and no claim

has been added. Claims 1-68 remain pending in the letter.

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

2.   Claims 1-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over by

Whitehouse (U.S. Patent No. 6,005,945) in view of Leon (U.S. Patent No. 6,424,954).

3.   As per claim 1, Whitehouse teaches a security system (*secure central computer, 102*) for

securing data in a computer network (*network 100, fig 3, 4, 7*) comprising a plurality of user

terminals (*customer, user, 102*) coupled (*connected*) to the computer network, a cryptographic

device (*cryptographic key*) remote from the plurality of user terminals and coupled to the

computer network, a plurality of security device transaction data for ensuring authenticity of the

one or more users, wherein each security device transaction data is related to a user (*see fig 3, 4*

and 7, column 8 line 30-9 line 63). Whitehouse fails to teach a cryptographic device includes a

computer executable code for authenticating one or more users and verifying that the

authenticated user is authorized to assume a role. However, Leon teaches a cryptographic device

includes a computer executable code for authenticating one or more users and verifying that the

authenticated user is authorized to assume a role (*see column 8 lines 45-67, 9 lines 20-27*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention

was made to modify Whitehouse's inventive concept to include Leon's cryptographic device

includes a computer executable code for authenticating one or more users and verifying that the

authenticated user is authorized to assume a role because this would have provided knowledge to

the system as to which entity is using the system in order to determine which key to load unto

system and which level of security is applicable.

4.   As per claim 2, Whitehouse teaches a system wherein the security device transaction data

related to a user is loaded into the cryptographic device when the user requests to operate on a

value bearing item (*see column 9 line 32-63*).

5.   As per claim 3, Whitehouse teaches the claim inventive concept stated in claim 1.

Whitehouse fails to teach a system wherein the assumed role includes one or more corresponding

operations to be performed by the authenticated user. However, Leon teaches a system wherein

the assumed role includes one or more corresponding operations to be performed by the

authenticated user (*see column 8 lines 45-62, 9 lines20-27, 35-67*). Therefore, it would have

been obvious to one of ordinary skill in that art at the time the invention was made to modify

Whitehouse's inventive concept to include Leon's system wherein the assumed role includes one

or more corresponding operations to be performed by the authenticated user because this would

have provided knowledge to the system as to which entity is using the system in order to

determine which key to load unto system and which level of security is applicable.

6.   As per claim 4-10, Whitehouse teaches Whitehouse teaches the claim inventive concept

stated in claim 1. Whitehouse fails to teach a system wherein the assumed role is a security

officer role to initiate a key management function, a key custodian role to take possession of

shares of keys, an administrator role to manage a user access control database, an auditor role to

manage audit logs, a provider role to withdraw from a user account, a user role to operate on a

VBI, a certificate authority role to allow a public key certificate to be loaded and verified.

However, Leon teaches a system wherein the assumed role is a security officer role to initiate a

key management function, a key custodian role to take possession of shares of keys, an

administrator role to manage a user access control database, an auditor role to manage audit logs,

a provider role to withdraw from a user account, a user role to operate on a VBI, a certificate

authority role to allow a public key certificate to be loaded and verified (*see column 8 lines 45-9

line 67)*. Therefore, it would have been obvious to one of ordinary skill in that art at the time the

invention was made to modify Whitehouse's inventive concept to include Leon's system wherein

the assumed role is a security officer role to initiate a key management function, a key custodian

role to take possession of shares of keys, an administrator role to manage a user access control

database, an auditor role to manage audit logs, a provider role to withdraw from a user account, a

user role to operate on a VBI, a certificate authority role to allow a public key certificate to be

loaded and verified because this would have provided knowledge to the system as to which

entity is using the system in order to determine which key to load unto system and which level of

security is applicable.

7.   As per claims 11-14, 16, Whitehouse teaches the inventive concept as stated in claim 1.

Whitehouse fails to teach a system wherein the cryptographic device includes a state machine for

determining a state corresponding to availability of one or more commands in conjunction with

the role, stateless, includes a computer executable code for preventing unauthorized modification

of data, for ensuring the proper operation of cryptographic security and VBI related meter

functions, for supporting multiple concurrent users and maintaining a separation of roles and

operations performed by each user. However, Leon teaches a system wherein the cryptographic

device includes a state machine for determining a state corresponding to availability of one or

more commands in conjunction with the role, stateless, includes a computer executable code for

preventing unauthorized modification of data, for ensuring the proper operation of cryptographic

security and VBI related meter functions, for supporting multiple concurrent users and

maintaining a separation of roles and operations performed by each user (*see column 8 lines 45-*

9 line 67). Therefore, it would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify Whitehouse's inventive concept to include Leon's system

wherein the cryptographic device includes a state machine for determining a state corresponding

to availability of one or more commands in conjunction with the role, stateless, includes a

computer executable code for preventing unauthorized modification of data, for ensuring the

proper operation of cryptographic security and VBI related meter functions, for supporting

multiple concurrent users and maintaining a separation of roles and operations performed by

each user because this would have provided knowledge to the system as to which entity is using

the system in order to determine which key to load unto system, which state to operate the

system and which level of security is applicable.

8.   As per claim 15, Whitehouse teaches a system wherein at least one of the users is an enterprise account *(see column 23 line 41-67)*.

9.   As per claim 17-18, Whitehouse teaches a system wherein the value bearing item is a mail piece comprises a digital signature *(fig 2)*.

10.   As per claim 19 and 20, Whitehouse teaches a system wherein the cryptographic device encrypts validation information according to a user request for printing a VBI, generates data sufficient to print a postal indicium in compliance with postal service regulation on the mail piece *(fig 2)*.

11.   As per claim 21 and 22, Whitehouse teaches a system wherein bar code is printed on the value bearing item that is a ticket *(fig 2)*.

12.   As per claim 23 and 24, Whitehouse teaches a system wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list, a private key, a public key, and a public key certificate, wherein the private key is used to sign device status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the device and the VBI are authentic *(see column 10 line 45-11 line 29, 20 line 16-40)*.

13.   As per claim 25, Whitehouse teaches a system further comprising at least one more

cryptographic device remote from the plurality of user terminals coupled to the computer

network, wherein the at least one more cryptographic device includes a computer executable

code for authenticating any of the plurality of users *(see figs 4, and 7)*.

14.   As per claim 26, Whitehouse teaches a system wherein the cryptographic device shares a

secret with the at least one more cryptographic device *(see column 8 lines 30-42, 9 lines 12-31,*

10 lines 50-11 line 29, 12 lines 35-64).

15.   As per claim 27-29, Whitehouse teaches a system wherein one of the plurality of

cryptographic devices is a master device and generates a master key set (MKS) includes a Master

Encryption Key (MEK) used to encrypt keys when stored outside the device and a Master

Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside

of the device exported to other cryptographic devices by any cryptographic device *(see column 4*

line 20-27, 16 lines 39-44, 23 lines 41-67).

16.   As per claim 30, Whitehouse teaches a method for securing data *(secure computer, 104,*

for securing data) in a computer network *(network, 100, fig 3 and 4)* having a plurality of user

terminals *(user, 102)*, the method comprising storing *(memory for storing, 154)* information

(user data) about a plurality of users using the plurality of terminals in a database remote from

the plurality of securing the information about the users in the database by one or more of

cryptographic devices *(cryptographic keys)* remote from the plurality of user terminals, storing a

plurality of security device transaction data *(transaction data)*, wherein each transaction data is

related to one of the plurality of users. Whitehouse fails to teach verifying that a user is

authorized to assume a role. However Leon teaches verifying that a user is authorized to assume

a role (*see column 8 lines 45-67, 9 lines 20-27*). Therefore, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to modify Whitehouse's inventive

concept to include Leon's verifying that a user is authorized to assume a role because this would

have provided knowledge to the system as to which entity is using the system in order to

determine which key to load unto system and which level of security is applicable.

17.   As per claim 31, Whitehouse teaches a method of loading a security device transaction

data related to a user into one of the one or more of cryptographic devices when the user requests

to operate on a value bearing item (*see column 9 line 32-63*).

18.   As per claim 32-40, Whitehouse teaches the inventive concept as stated in claim 1.

Whitehouse fails to teach a method of authenticating the identity of each user, verifying that the

user is authorized to perform a corresponding operation based on the assumed role wherein the

assumed role is a security officer role and the corresponding command is initiating a key

management function, a key custodian role to take possession of shares of keys, an administrator

role to manage a user access control database, an auditor role to manage audit logs, a provider

role to authorize increasing credit for a user account, a user role to perform expected IBIP meter

operation, a certificate authority role to allow a public key certificate to be loaded and verified.

However Leon teaches a method of authenticating the identity of each user, verifying that the

user is authorized to perform a corresponding operation based on the assumed role wherein the

assumed role is a security officer role and the corresponding command is initiating a key

management function, a key custodian role to take possession of shares of keys, an administrator

role to manage a user access control database, an auditor role to manage audit logs, a provider

role to authorize increasing credit for a user account, a user role to perform expected IBIP meter

operation, a certificate authority role to allow a public key certificate to be loaded and verified

(*see column 8 lines 45-9 line 67*). Therefore, it would have been obvious to one of ordinary

skill in the art at the time the invention was made to modify Whitehouse's inventive concept to

include Leon's a method of authenticating the identity of each user, verifying that the user is

authorized to perform a corresponding operation based on the assumed role wherein the assumed

role is a security officer role and the corresponding command is initiating a key management

function, a key custodian role to take possession of shares of keys, an administrator role to

manage a user access control database, an auditor role to manage audit logs, a provider role to

authorize increasing credit for a user account, a user role to perform expected IBIP meter

operation, a certificate authority role to allow a public key certificate to be loaded and verified

because this would have provided knowledge to the system as to which entity is using the system

in order to determine which key to load unto system, which state to operate the system and which

level of security is applicable.

19.   As per claim 41, Whitehouse teaches the inventive concept as stated in claim 1.

Whitehouse fails to teach a method of determining a state corresponding to availability of one or

more commands in conjunction with the roles. However, Leon teaches a method of determining

a state corresponding to availability of one or more commands in conjunction with the roles (*see

column 8 lines 45-62, 9 lines 35-67*). Therefore, it would have been obvious to one of ordinary

skill in the art at the time the invention was made to modify Whitehouse's inventive concept to

include Leon's a method of determining a state corresponding to availability of one or more

commands in conjunction with the roles this would have provided knowledge to the system as to which entity is using the system in order to determine which level of security is applicable.

20.   As per claim 43, Leon teaches a method wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state (*see column 9 lines 59-67*).

21.   As per claim 44, Whitehouse teaches a method of storing data for creating an indicium, account maintenance, and revenue protection (*see figs 4 and 7*).

22.   As per claim 45-47, Whitehouse teaches a method of printing a mail piece includes a digital signature, a postage amount, an ascending register of used postage and descending register of available postage (*see abstract, column 16 lines 25-38*).

23.   As per claim 48, 49, Whitehouse teaches a method of printing a ticket, a coupon (*see fig 2*).

24.   As per claim 50, Whitehouse teaches a method wherein the security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token, an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list (*see column 8 lines 30-42, 9 lines 12-31, 10 lines 50-11 line 29, 12 lines 35-64*).

25.   As per claim 51, Whitehouse teaches a method of using a private key to sign device

status responses and the VBI which, in conjunction with a public key certificate, demonstrates

that the device and the VBI are authentic *(see column 9 line 32-63)*.

26.   As per claim 52, Whitehouse teaches a method of sharing a secret with any of the other

devices *(see column 9 line 32-63)*.

27.   As per claim 53-56, Whitehouse teaches a method of generating a master key set (MKS),

generating a Master Encryption Key (MEK) used to encrypt keys when stored outside the device,

Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored

outside of the device and performing one or more of Rivest, Shamir and Adleman (RSA) public

key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number

generation algorithms by each of the cryptographic devices *(see column 4 line 20-27, 16 lines

39-44, 23 lines 41-67)*.

28.   As per claim 57, Whitehouse teaches a cryptographic device *(secure central computer,

102)* for securing data *(postal information)* on a computer network *(network 100, fig 3, 4)*

comprising a processor *(postal authority computer for processing, 180)* programmed to

authenticate *(authenticate)* a plurality of users *(users, 104)* on the computer network *(network

100, fig 3, 4)* for secure processing of a value bearing item *(postal indicium, fig 2) (see abstract,

figs 2, 3, 4)*, a memory *(memory, 154)* for storing *(stores)* security device transaction data

(records) for ensuring authenticity of a user, wherein the security device transaction data is

related to the one of the plurality of users, a cryptographic engine (*cryptographic key*) for

cryptographically protecting data and an interface (*interface, 152, 112, 252*) for communicating

with the computer network (*see abstract, fig 4, 7, column 8 lines 54-8 line 63*). Whitehouse fails

to teach a system wherein to determine that user is authorized to assume a role. However Leon

teaches a system wherein to determine that user is authorized to assume a role (*see column 8

lines 45-67, 9 lines 20-27*). Therefore, it would have been obvious to one of ordinary skill in the

art at the time the invention was made to modify Whitehouse's inventive concept to include

Leon's a system wherein to determine that user is authorized to assume a role because this would

have provided knowledge to the system as to which entity is using the system in order to

determine which key to load unto system and which level of security is applicable.

29.   As per claim 58-62, Whitehouse teaches the inventive concept stated in claim 1.

Whitehouse fails to teach a cryptographic device wherein the processor is programmed to

verify that the identified user is authorized to assume a role of a key custodian role to take

possession of shares of keys, an administrator role to manages a user access control database, a

provider role to authorize increasing credit for a user account or a user role to perform

expected IBIP postal meter operations and perform a corresponding operation. However, Leon

teaches a cryptographic device wherein the processor is programmed to verify that the

identified user is authorized to assume a role of a key custodian role to take possession of

shares of keys, an administrator role to manages a user access control database, a provider role

to authorize increasing credit for a user account or a user role to perform expected IBIP postal

meter operations and perform a corresponding operation (*see column 8 lines 45-9 line 67*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify Whitehouse's inventive concept to include Leon's a

cryptographic device wherein the processor is programmed to verify that the identified user is

authorized to assume a role of a key custodian role to take possession of shares of keys, an

administrator role to manages a user access control database, a provider role to authorize

increasing credit for a user account or a user role to perform expected IBIP postal meter

operations and perform a corresponding operation because this would have provided knowledge

to the system as to which entity is using the system in order to determine which level of security

is applicable.

30.   As per claim 63-65, Whitehouse teaches a cryptographic device further comprising a

stored secret that is a password, a public/private key for cryptographically protecting data (*see*

column 8 lines 30-42, 9 lines 12-31, 10 lines 50-11 line 29, 12 lines 35-64).

31.   As per claim 66, Whitehouse teaches a cryptographic device wherein the value bearing

item is a postage value including a postal indicium (*see abstract, column 16 lines 25-38).*

32.   As per claim 67-68, Whitehouse teaches a cryptographic device wherein the value

bearing item that include a bar code is a ticket (*fig 2).*

Response to Arguments

33.   Applicant's arguments filed October 29th, 2003 have been fully considered but they are

not persuasive.

a.   Applicants argues that the prior arts (Whitehouse and Leon) fail to teach among

other thing a cryptographic device includes a computer executable code for

authenticating one or more users and verifying that the authenticated user is authorized to

assume a role. Examiner respectfully disagrees with applicant's characterization of the

prior arts. Whitehouse teach among other things and end user computer typically includes

a data processor and a communication procedure for sending postage requests to a secure

central computer at which a user account has been established, and for receiving a

corresponding digital postage indicium. A postage indicium printing procedure prints a

postage indicium in accordance with the received digital postage indicium. Each postage

request will typically include a user account identifier that identifies a previously

established user account, a source address identifier indicating where a mail piece is to be

mailed from, a destination address identifier indicating where the mail piece is to be

mailed to, *authentication information for authenticating that the postage request is from*

an end user associated with the specified user account identifier (emphasis added). The

digital postal indicia will typically include data representing the user account identifier,

source address identifier, and destination address identifier in a corresponding on of the

postage requests. Leon discloses in the background of his disclosure the problem with

postage meters that have been dedicated, stand-alone devices, capable only of printing

postage indicia on envelopes (or labels, in the case of parcels). These devices normally reside at a single user location and only provide postage metering for that location. Such postage meters often require the user to physically transport the device to a post office for resetting (i.e., increasing the amount of postage contained in the meter). Leon's inventive concept solves this problem by creating a system that includes a postage metering system that includes a host PC, an SMD, and a printer. The host PC includes a user interface to receive postage information. The system postage metering system includes a postage metering device that couples to a host personal computer (host PC) via a communications link. Host PC couples to a system server via another communications link which can be a serial link, a telephone link, a wireless link, or other links, which indicates that the secure postage device is remotely located from the user. Metering device includes a secure meter device (SMD) responsible for maintaining the contents of certain security relevant data items (SRDIs).The SMD comprises a cryptographic module that performs the secure processing required by the postage metering system. The SMD supports the provider role by providing the following services: Registration, Funding, Audit, and Withdrawal. Whenever one of these services is requested, the SMD validates that the requester is an authorized provider. This is achieved by using the provider's public key to validate the signature on the service request that has been signed using the provider's private key. The provider's public key is retrieved from the Provider X.509 certificate that is loaded by the Crypto-Officer during initialization.

b.   In response to applicant's argument that there is no suggestion to combine the

references, the examiner recognizes that obviousness can only be established by

combining or modifying the teachings of the prior art to produce the claimed invention

where there is some teaching, suggestion, or motivation to do so found either in the

references themselves or in the knowledge generally available to one of ordinary skill in

the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*,

958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both references are in the

same technological art and furthermore on of ordinary skill in the art would find is

constructive and innovative to combine the concept of Whitehouse with Leon because it

would have provide a more secure remotely centralized system wherein both postage

accounting and security features are highly desirable. Such a system would allow the

printing of postage indicia at locations that are convenient to the end-user by allowing

the user to take a portion of the system to the item in need of postage, rather than the

reverse.

c.   In response to applicant's argument that the examiner's conclusion of obviousness

is based upon improper hindsight reasoning, it must be recognized that any judgment on

obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning.

But so long as it takes into account only knowledge which was within the level of

ordinary skill at the time the claimed invention was made, and does not include

knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper.

See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).
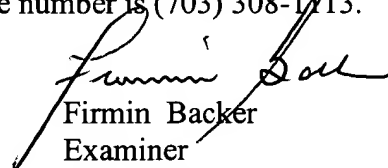
Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The

examiner can normally be reached on Mon-Thu 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, James Trammell can be reached on (703) 305-9768. The fax phone number for the

organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is (703) 308-1713.

Firmin Backer
Examiner
Art Unit 3621

December 4, 2003